



WASHINGTON, THE DISTRICT OF COLUMBIA

28 JAN 1985

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL
INSPECTOR GENERAL
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Automated Information Systems Security

I have reviewed the report prepared by Director, National Security Agency (DIRNSA), in coordination with Under Secretary of Defense for Research and Engineering (USDRE) and Under Secretary of Defense for Policy (USD(P)), that resulted from the examination of the policies, organizational arrangements, and programmatic aspects involved in automated information systems security. This examination was directed by my 12 January 1984 memorandum, same subject as above. As a result of my review of the report, I direct that the following actions be initiated:

(a) The USD(P) will:

- (1) in collaboration with the Computer Security Evaluation Center, prepare a revised DODD 5200.28 which will expand the scope of the present directive to include all computer-driven information systems and which will provide expanded policy guidance on mandatory statements of computer security requirements for all ADP procurements and the use of computer security guidelines and standards.
- (2) upon issuance of the Trusted Computer System Evaluation Criteria, revise DODD 5200.28 and 5100.55 to encourage system managers for US networks that interoperate with the systems of our allies to ensure that all components are evaluated by a common security criteria.

(b) The DIRNSA will:

- (1) establish an ad hoc working group to develop a common set of security criteria for use by all Designated Approving Authorities.
- (2) develop a Computer Security Vulnerability Reporting Program.

01433

- (3) continue the development of standard criteria and application guidance for network security.
- (4) prepare an advanced technology forecast, in coordination with Defense Advanced Research Project Agency (DARPA) and Office of the Under Secretary of Defense for Research and Engineering (Research and Advanced Technology) (OUSDRE(R&AT)) to assess the continuing applicability of security criteria to the emerging technology.
- (5) insure adequate resources are applied to the Computer Security Evaluation Center's primary mission of commercial computer security hardware/software product evaluation and focus on developing methods for reducing the manual level of effort currently required for these activities.

The initiation of these actions will significantly strengthen the Department's automated information system security. I have asked the Under Secretaries for Policy and Research and Engineering to continue to review the status of comprehensive DoD automated information system security efforts to ensure that security measures keep pace with the rapid proliferation of advanced information processing and network technologies.

